NMCI and its Management of the Step Sites

EWS 2003

Subject Area General

NMCI and its Management of the Step Sites
Contemporary Issues Paper

Student

Captain Anthony Michel
CG#3

Due Date

February 21, 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
NMCI and its Management of the Step Sites	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Marine Corps War College,Marine Corps University,Marine Corps Combat Development Command,Quantico,VA,22134-5067**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**10**	

Introduction

The Navy possesses obsolete information technology infrastructure and has about 1,000 networks, some without system security. Navy and Marine Corp Intranet (NMCI) is an enterprise-wide service contract, which was engaged to incorporate the newest strategic computing and communications capabilities. The Department of the Navy (DoN), Defense Information Systems Agency (DISA) and Department of Defense (DoD) are working with NMCI to improve security, standardize hardware, software and establish connectivity throughout the command, control, communication and computer information (C4I) network. Their goal is to provide online, anytime, and anywhere connectivity for voice, video, as well as data exchange between tactical/non-tactical forces for Naval and other DoD organizations. To achieve these goals, NMCI needs to control the step sites.

What are step sites?

Step sites are tactical entry points that provide access to the integrated tactical strategic data network (ITSDN). “The network provides an IP router based data network to support tactical/deployed forces” (MCWP 3-40.3 4-1). There are fourteen step sites established through out the world: Ft Belvoir, Va., Wahiawa, HI., Northwest, Va., Ft Buckner, Japan., Ft. Detrick,

MD., Riyadh, Saudi Arabia., Ft. Meade, MD., Landstuhl, Germany., Camp Roberts, CA., Croughton, UK., Ft. Bragg, NC., Bahrain., MacDill AFB, FL., and Lago Patria, Italy. These sites allow MAGTF's and other DoD organizations to successfully access or link both tactical and garrison networks from any deployment.

What is NMCI?

NMCI is the acronym for Navy and Marine Corp Intranet. According to the Department of the Navy, NMCI is the Navy's first step toward reaching both Joint Vision 2010 and Joint Vision 2020's goal of information superiority for the Department of Defense. According to Ormerod, NMCI "has been called the backbone of the revolution in military affairs". He goes on to state that information superiority is defined as "the ability to collect, process and disseminate an uninterrupted flow of information while denying the same to an adversary…. Coupled with the Navy's shipboard information technology for the 21st Century and the Marine Corp's Tactical Network (MCTN), NMCI will provide a standardize and worldwide reach-back capability for deployed forces" (Ormerod 4). Ultimately, NMCI will establish a standardized end-to-end communication system for all civilian and military personnel within the Department of the Navy. Replacing the Navy's numerous networks, NMCI will provide access, interoperability, and security to the Department of the Navy.

NMCI must comply with the following DoN guidelines: Information Technology Standards Guidance (ITSG), Information Program and Information Assurance/Computer Network Defense (IA/CND). Consequently, authorized DoN personnel are the approving authority for these NMCI sections: security architecture, security critical product selections, Network connectivity plan, Security procedures, and other security critical factors as required. However, the contractor is still responsible for the overall performance of the NMCI. The Marine Corps tactical Network (MCTN) will support deployed Marine Corps units, but NMCI will provide all other DoN requirements. Further, “under the service contract, the service provider owns and maintains all required desktop and network hardware and software, and provides all required IT services, including pier connectivity” (Ormerod 26).

Who controls the step sites

“The Defense Information Systems Agency (DISA) provides assistance and oversight in evaluating NMCI system objectives, reviewing implementation methodology, and reconciling development efforts with DoD IT guidelines.” Consequently, “DISA monitors all Worldwide Access Network (WAN) requirements and long haul services provisioning.” Furthermore, “DISA administers the Defense Information Systems Network (DISN),

which provides connectivity to other DoD and Governmental agency activities. NMCI interfaces directly with the DISN to transport voice, video, and data" (Ormerod, 8).

The DISN is the means to transport information between the tactical and garrison network. "As a first step in DISN implementation, DISA established the Integrated Tactical Strategic Data Network (ITSDN) to provide an IP router based data network to support deployed forces" (MCWP 6-22). To access the ITSDN, step sites were established. The Navy and DISA own these sites. Here are two organizations providing the same service under different control. However, to ensure interoperability, the Department of Defense mandates NMCI conformance with the following directives: Joint Tactical Architecture (JTA) and DII Common Operating Environment Level V. In fact, "DoD has placed considerable effort and resources into the development and implementation of numerous interoperable (joints) systems such as the Global Command and Control System (GCCS), the Joint Force Requirements Generator II (JFRG II), and the Joint Surveillance Target Attack Radar System (JSTARS)" (Ormerod 8). A secure environment for these systems was developed known as the Global Information Grid (GIG): "the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and

provide information on demand to war fighters, policy makers, and support personnel" (Ormerod 8).

Proposed control on step sites

According to the NMCI Report to Congress, there are two sets of integrated product teams that supervise the Navy Marine Corps Intranet. "The Action Collaboration Teams (ACT), which focus on the detailed technical and administrative functions and the Integrating Integrated Product Team (IIPT) and its Working Integrated Product Teams (WIPT), which concentrate on supervisory issues and ensuring appropriate risk mitigation" (1). These teams are made up of the intelligent individuals that do the work on both the civilian and military side. It also, has the senior level executive services that adjudicate decisions and disagreements. With this type of leadership already developed and operational, the NMCI could oversee the step sites that link both networks. All that remains is for NMCI to receive permission to assume control. In the past money has always been the problem that allowed certain organizations/units to upgrade their networks while others were left with second or even third generations equipments. With NMCI overseeing the networks, all organizations would be upgraded at the same time. There would be no new hardware or software introduced without properly being tested first and then fielded. The era of one

finding the answer while others were still looking would be over or at least diminished. A collective effort would be established to ensure everyone had the best hardware, software and solutions available. The same personnel would still be providing the service, but the cost could be spread across the DoD organization minimizing impact to individual budgets.

Counter arguments

Opponents to NMCI control of the step sites argue civilians should not be put in charge of warfighting capabilities because they do not have the same level of commitment. For example, contractors have specified hours to work and may not share the same desire of mission accomplishment. This author would argue that civilians would be the best people to run systems and equipment that connect the warfighter to the garrison capabilities and networks. Civilian contractors have and maintain access to the newest knowledge, information and equipment capabilities. They are driven by profit to provide customer service, which transcends rank. Ultimately, contractors are driven to support the customer's mission. Hence they do share mission accomplishment. The accountability differs in that it is profit versus rank. Service is defined by the contract not by the individual's rank or friendship. Moreover, using civilians would also increase reliability and

continuity in each job position. Civilians remain at jobs and locations longer than military personnel do. They do not have to transfer every few years to meet the rotation requirement.

Furthermore, the civilian contractors are supervised by military personnel and DoD representatives, which ensure that all requirements are met. As described earlier, the two teams that are overseeing NMCI are composed of military and civilian personnel to ensure the best capabilities and equipment are used effectively. DISA is the organization that DoD directed to watch and track NMCI installation. Even though NMCI would take over the step sites, the DISA personnel would still warrant that informational flow from the tactical environment to the garrison network.

Because NMCI is lead by the Navy, others also argue that USMC interests would be subject to naval control. Even though the Department of the Navy has the lead on NMCI, it is still a Department of Defense system and must respond to user needs. The Marine Corps has already initiated a means to fix its numerous hardware and software issues, but by allowing NMCI to provide a standard network throughout the DoD will improve communication between all services and organizations. If NMCI is not used, each organization will have to ensure their own upgrades and their maintenance personnel have the funds and

means to maintain proper educational standards. By allowing NMCI to maintain the step sites, DoD is guaranteeing that the individuals and equipment used would have the most available knowledge and training, the newest equipment, and most updated software out there.

Conclusion

It is easy to improve security, standardize hardware and software by purchasing the same equipment, and setting policy for all users. It is even possible to integrate all the networks with the new programs. However, data exchange between tactical/non-tactical Department of Defense organizations requires that the contractor maintains all hardware and software to standard and upgrade as new technology evolves. This ensures that NMCI does not fall behind the corporate America. Quality, however can be accomplished only if NMCI also controls the steps sites that will connect the Garrison network to the tactical/deployed network. It is only logical to have the same people controlling both networks' equipment.

Works Consulted

Department of the Navy. “Analysis of Alternatives.” Navy Marine Corps Intranet (NMCI) Report to Congress (n.p., Washington D.D. 30 June 2000).

Department of the Navy. “Executive Summary.” Navy Marine Corps Intranet (NMCI) Report to Congress (Washington DC, 30 June 2000).

Department of the Navy Information Management & Information Technology (DoN IM/IT) Pamphlet. Catalog of DoN IM/IT Strategic Goals, Tools and Training (n.p., July 2000)

Deputy Assistant to the Secretary of the Navy for C4I/EW/Space. Navy Marine Corps Intranet (NMCI) Execution. 19 December 2000. 1.

Electronic Data Systems. “About EDS,” URL: http://www.eds.com/about_eds/en_about_eds.shtml, viewed 10 January 2003.

Joint Chiefs of Staff Joint Pub 1-02. Department of Defense Dictionary of Military and Associated Terms (Washington, DC: GPO, 10 June 1998).

Joint Vision 2020. (Washington, DC: US Government Printing office, June 2000).

Marine Corp Warfighting Publication. “Communciations and Information Systems,” (Washington, DC: GPO, 16 November 1998).

Gerald J. Ormerod, “Outsourcing information Technology Services within the DoD”, 2001

Role of IPTs in NMCI, URL: http://164.224.120.151/congress/2-J_Role_of_IPTs_in_NMCI.pdf, viewed 11 January 2003.